Cours 3 – Hack

Quand il clique sur le div, mais enfaite il a mit un iframe par dessu, mais avec une opaciter de 0 donc tu ne le vois pas. 🡪 CLICK JAGGING



Les navigateurs trouvent sa louche si l opaciter est a 0, mais a 0.1 pas trop.

Comment se protéger du click jagging 🡪 cela prends un petit code javascript

Busting : un petit code a rentrer en js

If url {

top.location.href = location.href

}

Pour verifier si c est le url principal, si t es l url principal alors tu vas devenir la page principale du navigateur

Suite….

CSRF 🡪 je comprends que sur un onlget tu es connecter, mais je vais cacher un formulaire ou une image fausse pour faire une action dans le premier onglet, le premier site vas se connecter, faire des transactions etc. Donc résumer, il vas cliquer sur l image mais ca vas faire une autre action cacher.

Maintenant c est pas un hack populaire car ca n envoie plus les cookies, mais il existe des technique pour baypass.

Suite…

Dans chaque formulaire pour transaction on se déconnecter ou modifider la bd ou le compte dans chacun des formes tu vas ajotuer des tokens lavaleur de se token vas varier a chaque fois que je me connecte, donc a chaque fois que je me connecte ca vas me donner un nouveau token, mais a chaque fois que il y a une nouvelle session c est un nouveau. Si on essaie de faire un sign in, le hackeur ne pourra pas savoir si c est un token valide.

Brute force attack 🡪

Essayer toutes les combinaisaons possible justqua tant que sa vas marcher

Sha1 est trop rapide donc vaut mieux utiliser bycrypt qui est plus lent.

Prends tous les processeur de ton proc 🡪 plus rapide

Si le site met une sorte de verrouillage alors on pourrait plus faire un brute attack.

Prendre les mots de passe les plus utiliser.

Suite …

DDOS 🡪

200 000 ordinateur qui font des requetes et crash le site ou tu me donne 1 million, si je te met down ta reputation etc etc. Mais, j accepte que tu me met down, mais le buisiness vas mal marcher

Suite…

Tu peux mettre une du php dans le png et ouvrire un fichier dir et supprimer des fichiers genre

XSi : Pousser du scode dans le div input, et je stock dans la db mais la personne qui vas reload vas exécuter le script

Donc si tu met un script avec un href ca vas te href vers un link

Comment se protéger strp.tags, <script> &i8; script>